

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. **(Cancelled)**

2. **(New)** A method for transmitting an encrypted message from a first transmitter-receiver to a second transmitter-receiver, forming a communicating pair, the method comprising the steps of:

(a) encrypting, by the first transmitter-receiver using a first encryption device, a previous transmission received from the second transmitter-receiver;

(b) encrypting, by the first transmitter-receiver using said first encryption device, a reference to a previous transmission sent to the second transmitter-receiver;

(c) sending, by the first transmitter-receiver, said encrypted previous transmission and said encrypted reference to the second transmitter-receiver;

(d) receiving, by the second transmitter-receiver, said encrypted previous transmission and said encrypted reference;

(e) discovering, by the second transmitter-receiver, said first encryption device;

(f) decrypting, by the second transmitter-receiver using said first encryption device, said encrypted reference;

(g) decrypting, by the second transmitter-receiver using said first encryption device, said encrypted previous transmission;

(h) accessing, by the second transmitter-receiver, said encrypted previous transmission;

(i) encrypting, by the second transmitter-receiver using said first encryption device, said previous transmission;

(j) sending, by the second transmitter-receiver, said encrypted previous transmission to the first transmitter-receiver;

(k) receiving, by the first transmitter-receiver, said encrypted previous transmission;

(l) decrypting, by the first transmitter-receiver using said first encryption device, said encrypted previous transmission;

26 (m) confirming, by the first transmitter-receiver, the correctness of said previous
transmission;

28 (n) reporting, by the first transmitter-receiver, confirmation of said previous
transmission to the second transmitter-receiver; and

30 (o) encrypting, by the first transmitter-receiver using said first encryption device, a
current message.

3. (New) The method according to claim 2 further comprising the steps of:

2 selecting randomly said first encryption device from a group consisting of a plurality of
pseudo-random number generators, a plurality of elliptic curve cryptosystems, a plurality of
4 discrete-logarithm (RSA) cryptosystems, and a plurality of symmetric-key cryptosystems.

4. (New) The method according to claim 2 further comprising the steps of:

2 selecting said previous transmission received from the second transmitter-receiver from a
group consisting of a last message sent by the second transmitter-receiver, a predetermined
4 portion of the last message sent by the second transmitter-receiver, and a prespecified internal
data that is generated by the communicating pair that is independent of message content.

5. (New) The method according to claim 2 further comprising the steps of:

2 selecting said previous transmission sent to the second transmitter-receiver from a group
consisting of a previous referenced message sent to the second transmitter-receiver, a
4 predetermined portion of a previous referenced message sent to the second transmitter-receiver,
and a prespecified internal data that is generated by the communicating pair that is independent
6 of message content.

6. (New) The method according to claim 2 wherein said discovering step (e) further
2 comprises the step of:

using sequentially, by the second transmitter-receiver, each of a plurality of
4 cryptographic devices of the second transmitter-receiver, to attempt to decrypt said reference to a
previous transmission sent to the second transmitter-receiver until said reference to a previous
6 transmission is recovered, thus identifying said first encryption device.

7. (New) The method according to claim 6 further comprising the steps of:

2 after discovering said first encryption device, challenging the first transmitter-receiver by
the second transmitter-receiver to further provide evidence of an authenticity of the first
4 transmitter-receiver.

8. (New) The method according to claim 2 further comprising the steps of:

2 sending, by the first transmitter-receiver, said encrypted current message to the second
transmitter-receiver.

9. (New) A method for transmitting an encrypted message from a first transmitter-
2 receiver to a second transmitter-receiver, forming a communicating pair, the method comprising
the steps of:

4 (a) furnishing the communicating pair with a plurality of cryptographic devices for
encrypting and decrypting a message to be exchanged between the communicating pair;

6 (b) collaborating by the first transmitter-receiver with the second transmitter-receiver
to establish a one-time cryptographic pad for encrypting said message, said collaborating further
8 comprising:

(b1) exchanging information regarding internal data, as stored in internal data
10 structures, and states that are private and common to the communicating pair and are
independent of the content of transmitted messages; and

12 (b2) negotiating an agreement on a cryptographic device from said plurality of
cryptographic devices to be used to encrypt and decrypt said message; and

14 (c) preparing, by the first transmitter-receiver, the message for transmission by
encrypting said message with said cryptographic device.

10. (New) The method according to claim 9 wherein said negotiating step (b2) further
2 comprising the step of:

selecting said cryptographic device from said plurality of cryptographic devices from a
4 group consisting of a plurality of pseudo-random number generators, a plurality of elliptic curve
cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a plurality of
6 symmetric-key cryptosystems.

11. (New) The method according to claim 9 further comprising the steps of:

2 sending, by the first transmitter-receiver, said encrypted message to the second
transmitter-receiver.

12. (New) A communicating pair system, the system comprising:

2 a first transmitter-receiver having a first encryption device;

 a second transmitter-receiver in communication with said first transmitter-receiver;

4 a previous transmission received by said first transmitter-receiver from said second
transmitter-receiver, wherein said first transmitter-receiver encrypts said previous transmission
6 with said first encryption device; and

 a reference to a previous transmission sent to said second transmitter-receiver by said
8 first transmitter-receiver, wherein said first transmitter-receiver encrypts said reference to a
previous transmission with said first encryption device, and said first transmitter-receiver sends
10 said encrypted previous transmission and said encrypted reference to a previous transmission to
said second transmitter-receiver;

12 wherein said second transmitter-receiver discovers said first encryption device and,
utilizing said first encryption device, said second transmitter-receiver decrypts said encrypted
14 reference to a previous transmission and decrypts said encrypted previous transmission, accesses
said previous transmission, encrypts said previous transmission with said first encryption device,
16 and sends said encrypted previous transmission to said first transmitter-receiver, where said first
transmitter-receiver decrypts said encrypted previous transmission with said first encryption
18 device and confirms the correctness of said previous transmission, reports said confirmation to
said second transmitter-receiver, and encrypts a current message with said first encryption
20 device.

13. (New) The system according to claim 12 wherein said first encryption device is
2 selected from a group consisting of a plurality of pseudo-random number generators, a plurality
of elliptic curve cryptosystems, a plurality of discrete-logarithm (RSA) cryptosystems, and a
4 plurality of symmetric-key cryptosystems.

14. (New) The system according to claim 12 wherein said previous transmission
2 received by said first transmitter-receiver is selected from a group consisting of a last message
sent by the second transmitter-receiver, a predetermined portion of the last message sent by the

- 4 second transmitter-receiver, and a prespecified internal data that is generated by the communicating pair that is independent of message content.

15. **(New)** The system according to claim 12 wherein said reference to a previous
2 transmission sent to the second transmitter-receiver is selected from a group consisting of a
previous referenced message sent to the second transmitter-receiver, a predetermined portion of a
4 previous referenced message sent to the second transmitter-receiver, and a prespecified internal
data that is generated by the communicating pair that is independent of message content.

16. **(New)** The system according to claim 12 wherein said first transmitter-receiver sends
2 said encrypted current message to said second transmitter-receiver.